

REMARKS

This Application has been carefully reviewed in light of the Final Office Action mailed on September 8, 2006 ("Office Action"). Claims 1-37 and 39 are pending in the Application. The Office Action rejects Claims 1-37 and 39. Applicants have cancelled Claims 1 and 11.

Overview:

The Office Action rejects claims over various combinations of references. As discussed below in detail, each of these rejections of the pending claims is incorrect. Example reasons why each of these rejections is incorrect are provided in summary form here, with additional details regarding why the assertions made in the Office Action are incorrect.

Applicants note that the amendment of Claim 2 should be entered because it merely rewrites the claim in independent form and addresses an informality in the claim previously recognized by neither the Applicants or the PTO. The amendment of Claim 13 should be entered because it merely rewrites the claim in independent form. However, even if such amendments were not entered, which would be improper, the remaining claims (including Claims 2 and 13 as unamended) are clearly allowable, and Applicants contend their rejection would not be upheld by a pre-appeal brief panel review.

- Independent Claim 2 is allowable at least because the combination of *Vaidya* and *Perelson* fails to disclose, expressly or inherently, "generating, for each of the modified signature definitions, a revised inspector instance based on the modified signature definition and the corresponding generated inspector instance."
- Independent Claim 13 is allowable at least because the combination of *Vaidya* and *Perelson* fails to disclose, expressly or inherently, "automatically generating, for each custom signature, executable code operable to detect intrusions associated with the custom signature based on the generated executable code of an associated default signature."
- Independent Claim 28 is allowable at least because the combination of *Vaidya* and *Perelson* fails to disclose, expressly or inherently, "a configuration handler

comprising: a default signature file storing one or more signature definitions defining one or more respective default signatures for use by the sensor; and a user signature file storing a plurality of user-defined signatures for use by the sensor.”

- Independent Claim 19 is allowable at least because the combination of *Chen* and *Kouznetsov* fails to disclose, expressly or inherently, “receiving from the sensor data indicative of parameters and associated values for the signature to be modified.”
- Independent Claim 19 is further allowable at least because the combination of *Chen* and *Kouznetsov* fails to disclose, expressly or inherently, “providing to the sensor a modified value for at least one of the parameters to create a modified signature.”
- Independent Claim 36 is allowable at least because the combination of *Vaidya* and *Bardsley* fails to disclose, expressly or inherently, “the signature definitions comprising: an engine parameter and an associated name for the engine parameter.”

Rejections Under 35 U.S.C. § 103(a):

The Office Action rejects Claims 1-6, 8, 10, 11, 13-18, 28 and 31-34 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,279,113 issued to Vimal Vaidya (“*Vaidya*”) in view of U.S. Patent No. Re 36,417 issued to Alan S. Perelson, et al. (“*Perelson*”). The Office Action rejects Claims 7 and 9 under 35 U.S.C. §103(a) as being unpatentable over *Vaidya* in view of *Perelson*, and further in view of U.S. Patent No. 5,557,742 issued to Smaha, et al (“*Smaha*”). The Office Action rejects Claims 12 and 29 under 35 U.S.C. §103(a) as being unpatentable over *Vaidya* in view of *Perelson*, and further in view of U.S. Patent No. 6,484,315 issued to Kevin J. Ziese (“*Ziese*”). The Office Action rejects Claim 30 under 35 U.S.C. §103(a) as being unpatentable over *Vaidya* in view of *Perelson*, further in view of *Ziese*, and further in view of *Smaha*. Applicants respectfully traverse these rejections.

Independent Claim 2 is allowable at least because the combination of *Vaidya* and *Perelson* fails to disclose, expressly or inherently, “generating, for each of the modified signature definitions, a revised inspector instance based on the modified signature definition and the corresponding generated inspector instance.” The Office Action relies on column 6,

lines 6-24 of *Perelson* as disclosing this limitation. *See* Office Action, page 11. However, this reliance is misplaced. For example, this passage merely discloses various formulas:

$$\begin{aligned} N_R &= \frac{\ln P_f}{\ln(1 - P_M)} \\ \text{since } f &\text{ is approximately } e^{-P_M N_S} = (1 - P_M)^{N_S} \\ -P_M N_S &= N_S \ln(1 - P_M) \\ \text{or} \\ -P_M N_S &= N_S \ln(1 - P_M) \\ \text{or} \\ N_R &= \frac{\ln P_f}{-P_M} = \frac{-\ln P_f}{P_M} \end{aligned}$$

Furthermore, *Perelson* clearly discloses that these formulas merely determine the “probability of a match” between the test string and the original string. *See Perelson*, column 5, lines 37-38. Therefore, *Perelson* fails to disclose, expressly or inherently, “generating, for each of the modified signature definitions, a revised inspector instance based on the modified signature definition and the corresponding generated inspector instance.” Thus, the combination of *Vaidya* and *Perelson* fails to disclose, expressly or inherently, the limitations of Claim 2.

For at least this reason, Independent Claim 2 is allowable, as are Claims 3-10 that depend therefrom. Reconsideration and favorable action are requested.

Independent Claim 13 is allowable at least because the combination of *Vaidya* and *Perelson* fails to disclose, expressly or inherently, “automatically generating, for each custom signature, executable code operable to detect intrusions associated with the custom signature based on the generated executable code of an associated default signature.” The Office Action relies on column 6, lines 6-24 of *Perelson* as disclosing this limitation. *See* Office Action, page 12. However, this reliance is misplaced. For example, this passage, as shown above in regard to Independent Claim 2, merely shows various formulas that determine the “probability of a match” between the test string and the original string. Therefore, *Perelson* fails to disclose, expressly or inherently, “automatically generating, for each custom signature, executable code operable to detect intrusions associated with the custom signature based on the generated executable code of an associated default signature.” Thus, the combination of *Vaidya* and *Perelson* fails to disclose, expressly or inherently, the limitations of Dependent Claim 13.

For at least this reason, Independent Claim 13 is allowable, as are Claims 12 and 14-18 that depend therefrom. Reconsideration and favorable action are requested.

Independent Claim 28 is allowable at least because the combination of *Vaidya* and *Perelson* fails to disclose, expressly or inherently, “a configuration handler comprising: a default signature file storing one or more signature definitions defining one or more respective default signatures for use by the sensor; and a user signature file storing a plurality of user-defined signatures for use by the sensor.” The Office Action relies on column 6, lines 53-57 of *Vaidya* as disclosing this limitation. *See* Office Action, page 9. However, this reliance is misplaced. For example, this passage expressly discloses:

Upon receiving a set or sets of attack signature profiles, each data collector 10 stores the set or sets of profiles it receives from the data repository 12 in its signature profile memory 39.

Thus, although each data collector has a signature profile memory for storing attack signature profiles, it does not have more than one signature profile memory. Therefore, even if the Office Action is correct in relying on *Vaidya* as disclosing either a default signature file or a user signature file, which Applicants do not address, *Vaidya* fails to disclose both. As a result, *Vaidya* fails to disclose, expressly or inherently, “a configuration handler comprising: a default signature file storing one or more signature definitions defining one or more respective default signatures for use by the sensor; and a user signature file storing a plurality of user-defined signatures for use by the sensor.” Thus, the combination of *Vaidya* and *Perelson* fails to disclose, expressly or inherently, the limitations of Independent Claim 28.

For at least this reason, Independent Claim 28 is allowable, as are Claims 29-34 that depend therefrom. Reconsideration and favorable action are requested.

The Office Action rejects Claims 19-27 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,960,170 issued to Eva Chen, et al. (“*Chen*”) in view of U.S. Patent No. 6,725,377 issued to Kouznetsov (“*Kouznetsov*”). Applicants respectfully traverse these rejections.

Independent Claim 19 is allowable at least because the combination of *Chen* and *Kouznetsov* fails to disclose, expressly or inherently, “receiving from the sensor data indicative of parameters and associated values for the signature to be modified.” The Office Action relies on column 7, lines 39-67 of *Kouznetsov* as disclosing this limitation. *See* Office Action, page 18. However, this reliance is misplaced. For example, this passage clearly discloses that the information sent is merely identification information:

This information includes: 1) the IP address 212 of anti-intrusion monitor server 202; and 2) a unique user ID attributable to anti-intrusion monitor server 202 (e.g. "TSMITH001199").

Identification information for a server is not, however, data indicative of parameters and associative values for the signature to be modified. Therefore, *Kouznetsov* fails to disclose, expressly or inherently, "receiving from the sensor data indicative of parameters and associated values for the signature to be modified." Thus, the combination of *Chen* and *Kouznetsov* fails to disclose, the limitations of Independent Claim 28.

Independent Claim 19 is further allowable at least because the combination of *Chen* and *Kouznetsov* fails to disclose, expressly or inherently, "providing to the sensor a modified value for at least one of the parameters to create a modified signature." The Office Action relies on column 7, lines 34-40 of *Chen* as disclosing this limitation. *See* Office Action, page 18. However, this reliance is misplaced. For example, this passage discloses creating an additional virus detection object:

After receipt of the virus detection object, in step 220 the virus detection object is executed by the client 300 and in step 225 the results of virus detection object execution are transmitted to the virus detection server 400 which receives the results and in step 230 produces an additional virus detection based upon the result of the execution of the first virus detection object.

(emphasis added). However, despite disclosing an additional virus detection object, the passage fails to disclose a modified signature. For instance, the Office Action uses the "virus signatures" at column 3, lines 57-59 of *Chen* as disclosing signatures. *See* Office Action, page 18. Instead of disclosing a modified virus signature, *Chen* merely discloses an additional virus detection object, and as seen at column 3, lines 57-63 of *Chen*, virus signatures are not virus detection objects, they merely help create virus detection objects:

Similarly, the virus pattern module and the virus rules module respectively includes groups of virus signatures and groups of rules that can be separately accessed. The iterative virus detection module operates in conjunction with the scanning module, the virus pattern module, and the virus rules module to produce virus detection objects.

(emphasis added). Therefore, because a virus signature is not a virus detection object, even if the Office Action is correct in relying on the virus signature of *Chen* as disclosing a signature, which Applicants do not address here, an additional virus detection object cannot

be a modified signature. As a result, *Chen* fails to disclose, expressly or inherently, “providing to the sensor a modified value for at least one of the parameters to create a modified signature.” Thus, the combination of *Chen* and *Kouznetsov* fails to disclose, the limitations of Independent Claim 19.

For at least these reasons, Independent Claim 19 is allowable, as are Claims 20-27 that depend therefrom. Reconsideration and favorable action are requested.

The Office Action rejects Claims 35-37 and 39 under 35 U.S.C. § 103(a) as being anticipated by *Vaidya* in view of U.S. Patent No. 2003/0061514 issued to Bardsley (“*Bardsley*”). Applicants respectfully traverse these rejections.

Independent Claim 36 is allowable at least because the combination of *Vaidya* and *Bardsley* fails to disclose, expressly or inherently, “the signature definitions comprising: an engine parameter and an associated name for the engine parameter.” The Office Action relies on the passage at page 3, paragraphs 0024-0030 of *Bardsley* as disclosing this limitation. *See* Office Action, page 23. However, this reliance is misplaced. For example this passage discloses:

Within the signature sets 301 through 303 of FIG. 3, the signature events 301B through 303B may include bit patterns or other identifiers suggestive of attempted intrusions. For example, one of the signature events 301B through 303B might be a bit pattern associated with the event “Protocol violation 3” that is know to be a prelude to a denial-of-service attack. Another of the signature events 301B through 303B might be a bit pattern associated with the event “arrival of a message from source ID aaa.bbb.ccc.ddd,” where the specified source ID is known to have been used in the past by a hacker.

(emphasis added). Although the passage discloses example names of events associated with the signature event, the passage does not disclose the name of the signature event. Furthermore, as clearly seen in Figure 3, *Bardsley* discloses a signature event, but fails to disclose the name of the signature event. As a result, even if the Office Action is correct in relying on *Bardsley* as disclosing an engine parameter, which Applicants do not address here, *Bardsley* fails to disclose the name of the engine parameter. Therefore, *Bardsley* fails to disclose, expressly or inherently, “the signature definitions comprising: an engine parameter and an associated name for the engine parameter.” Thus, the combination of *Vaidya* and *Bardsley* fails to disclose the limitations of Independent Claim 36.

For at least this reason, Independent Claim 36 is allowable, as are Claims 37 and 39 that depend therefrom. For analogous reasons, Independent Claim 35 is allowable. Reconsideration and favorable action are requested.

CONCLUSION

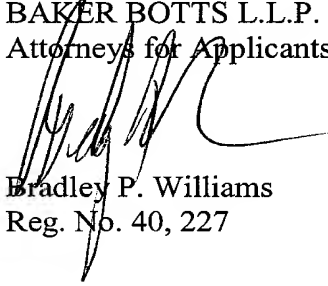
Applicants have now made an earnest attempt to place this case in condition for immediate allowance. For the foregoing reasons and for other apparent reasons, Applicants respectfully request allowance of all pending claims.

If the Examiner feels that prosecution of the present Application may be advanced in any way by a telephone conference, the Examiner is invited to contact the undersigned attorney at 214-953-6447.

Applicants believe no fee is due. However, if a fee is required, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 02-0384 of Baker Botts L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicants



Bradley P. Williams
Reg. No. 40, 227

Date: November 8, 2006

Correspondence Address:

2001 Ross Avenue
Dallas, Texas 75201-2980
Telephone 214.953.6447
Facsimile 214.661.4447

Customer Number: **05073**